

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

**SUSAN TAYLOR, individually and on behalf of
all others similarly situated,**

Plaintiff,

v.

VERIZON COMMUNICATIONS INC.,

Defendant.

Civil Action No. _____

JURY TRIAL DEMANDED

COMPLAINT

Plaintiff, Susan Taylor (“Plaintiff”), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Verizon Communications Inc., (“Defendant”) to obtain damages, restitution, and injunctive relief for the Class, later defined, from Defendant. Plaintiff makes the following allegations upon personal knowledge as to Plaintiff’s own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by counsel and the facts that are a matter of public record:

SUMMARY OF ACTION

The mobile advertising ecosystem unjustly rewards Defendant, at the expense of its wireless customers. For instance, by tracking mobile device activity, browsing history, location, purchases, and other private details, Defendant can monetize the data by selling it to third parties or otherwise use the data to serve targeted advertisements. Unfortunately, Defendant has either disclosed or permitted the collection of intimate details about its customers without giving them

an opportunity to consent to the collection or giving them a meaningful choice regarding the collection, use, disclosure, or deletion of their personal information.

Defendant's customers lacked any ability to consent to these data collection practices because the cookies, application programming interfaces (APIs), pixels, or other technology powering this advertising ecosystem took place behind the scenes and was not readily discoverable. By using or permitting the use of these tracking technologies, Defendant intentionally intruded upon the seclusion of its customers' private concerns or otherwise compelled its customers to unknowingly permit an inspection of their personal affairs. The unauthorized disclosure of customer information constitutes an invasion of a legally protected privacy interest, that is traceable to the Defendant's surreptitious surveillance of its customers and has resulted in actual, particularized, and concrete harm.

Therefore, Plaintiff, individually and on behalf of all others similarly situated, brings this class action against Defendant for the invasion of its customers' privacy by collecting, disclosing, and/or selling Customer Proprietary Network Information (CPNI) to unknown third-party advertisers without obtaining its customers' prior affirmative consent. Plaintiff brings this action to enforce fundamental privacy rights and to recover damages, in an amount to be determined at trial, attorneys' fees, and costs. Furthermore, Plaintiff seeks equitable or declaratory relief pronouncing Defendant's surreptitious surveillance of its customers is unlawful and antipodean to the public interest. Defendant should be required to implement meaningful guardrails on its commercial surveillance activities.

PARTIES, JURISDICTION & VENUE

1. Plaintiff, Susan Taylor is a resident and citizen of Jonesboro, Georgia. Plaintiff Taylor is a current Verizon wireless customer and has used Defendant's wireless network, devices, and mobile apps for about 12 years.

2. Defendant, Verizon Communications Inc., is a Delaware formed corporation, with a principal place of business located at 1095 Avenue of the Americas, New York, NY 10036. Defendant provides communications, technology, information, and entertainment products and services.

3. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. §1332, because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from each Defendant.

4. This Court has jurisdiction over Defendant as Defendant maintains its corporate headquarters in this District.

5. Venue is proper under 28 U.S.C §1391(b) because Defendant resides within this District, is subject to the court's personal jurisdiction, and maintains its principal place of business within this District.

STATEMENT OF FACTS

6. Defendant provides communications services through its wireless networks, as well as related equipment and wireless-enabled connected devices. In addition, Defendant offers various mobile applications to its subscribers, which are preloaded on Verizon devices.

7. Through the software preloaded onto its smartphones, tablets, smart watches, and mobile apps, Defendant collected information that relates to the quantity, technical configuration,

type, destination, location, and amount of use of a telecommunications service subscribed to by its customers.

8. By virtue of this carrier-customer relationship, Defendant allowed third parties to access information about its customers' activity on their mobile device and/or disclosed customer information to advertising companies using a variety of tracking technologies.

9. Defendant permitted advertising companies to use the information they collected to create mobile advertising identifiers associated with each customer's device. These companies were permitted to combine this information with information they collected elsewhere to create custom audiences for targeted ads. Customers were *automatically* included in this process and could not be removed from the program unless they opted out.

10. Defendant disclosed customer information it obtained by virtue of the carrier-customer relationship to third-party advertisers without obtaining consent. Defendant never informed customers as to how Defendant would share, use, and monetize their data prior to disclosing the data.

11. Plaintiff Taylor has been a wireless customer of Defendant for about 12 years. Plaintiff Taylor purchased a Samsung Galaxy S22 phone from Defendant about two years ago. All the phones Plaintiff has owned over the last six (6) years have been Samsung Galaxy phones.

12. Over the years, each phone Plaintiff Taylor owned came preloaded with various mobile apps including, but not limited to, VZNavigator and My Verizon. Currently, Plaintiff Taylor uses Verizon Cloud, Verizon Protect, Verizon Call Filter, and My Verizon.

13. In addition to Defendant's preloaded mobile apps, she has downloaded or used mobile gaming apps, health/wellness apps (e.g., Samsung Health), social media apps (e.g., Facebook, Instagram, Threads, TikTok), and navigation apps (e.g., Google maps, Waze).

14. In addition to the mobile apps mentioned above, Plaintiff Taylor regularly uses her mobile phone for online shopping. When using her mobile device for gaming or web surfing, she is frequently shown advertising. Plaintiff Taylor has noticed that after she has visited a certain store or searched for a product online using her mobile phone, ads related to items she has searched for or from retailers near places she has visited are displayed on her mobile device.

15. Upon information and belief, Defendant has tracked, compiled, and analyzed Plaintiff's web browsing, device location, mobile app usage, and other activity, both on and offline, and used this information to create a profile on her. On information and belief, Defendant continues to track Plaintiff Taylor's activity and make her personal information available to third parties without her consent. On information and belief, Plaintiff Taylor's electronic communications, including her internet activity and interaction with various mobile apps, were intercepted using cookies, application programming interfaces (APIs), pixels, or other technology, as described below.

16. Plaintiff Taylor was never given an opportunity to consent to the Defendant's sharing of her confidential information, including location data, with third parties for advertising purposes. Plaintiff Taylor does not know what information Defendant has collected about her during the 12-year relationship. Likewise, Plaintiff Taylor does not know what information Defendant permitted third parties to access and/or identify her, her mobile device, the websites she has visited, the purchases she has made, or other activity conducted through her mobile device.

17. As a result of Defendant's unauthorized actions, Plaintiff Taylor has spent time and effort attempting to understand the choices she has regarding interest-based advertising. Plaintiff Taylor would like to remove her information from the various advertisers and data brokers that

have received her information. Plaintiff Taylor continues to spend time and effort to understand and remedy the unauthorized disclosure of her personal information for advertising purposes.

18. Through this action, Plaintiff and Class Members seek damages for the losses suffered because of Defendant's misconduct, as well as injunctive relief aimed at deterring Defendant from engaging in such practices in the future. The putative Class is comprised of millions of Defendant's wireless customers who were not provided an opportunity to consent to the surreptitious collection and disclosure of their personal information for marketing and advertising purposes.

[A] Defendant failed to obtain consent prior to disclosing CPNI to advertising companies.

19. Defendant provides fixed wireless access (FWA) broadband through its wireless networks, as well as related equipment and devices, such as smartphones, tablets, smart watches, and other wireless-enabled connected devices.

20. Defendant also provides various mobile applications to its subscribers, which are often preloaded on Verizon devices. For example, the My Verizon app is a free account management tool available to all customers. Another example of a preloaded app is VZ Navigator, which provided turn-by-turn navigation, traffic data, weather, points of interest, and roadside assistance. A subscription to the VZ Navigator app cost about \$9.99 per month for unlimited access or \$2.99 for a one-day/24-hour use on select devices.

21. Whenever customers use their mobile devices, Defendant collected certain information about those customers including, but not limited to, information about: (i) how the customer used Defendant's services; (ii) how the customer used websites and mobile apps; and (iii) the location of the customer's wireless devices.

22. For example, Defendant's "Custom Experience" program collected information about websites its customers visited and the apps they used on their mobile devices to help Defendant personalize its marketing efforts and/or market new products and services. Customers were automatically included in the Custom Experience program and could not be removed from the program unless they opted out.

23. Additionally, Defendant allowed various advertising companies to collect, information about its customers' activity both on and off Defendant's websites and mobile apps.

24. More specifically, Defendant disclosed to advertisers, data brokers, and other third parties, sensitive location data tied to its mobile devices.

25. A mobile advertising ID (MAID) is, essentially, a digital fingerprint for mobile devices. These identifiers allow for data collection regarding mobile app usage and browsing behaviors to serve targeted advertisements.

26. A significant benefit of MAIDs is that advertisers can recognize the same user across multiple devices. This allows advertisers to track mobile app users, create custom audiences, and build more comprehensive profiles of user demographics, interests, and behaviors.

27. Notably, emerging technologies like machine learning, artificial intelligence and geofencing can enhance the precision of targeting. Geofencing, for example, leverages location-based technology (GPS or RFID) to deliver personalized messaging and advertising to customers.

28. Geofencing employs virtual "fences" or perimeters to identify users who enter or exit a specific location (retail stores, events, places of worship, hospitals, etc.). Once a specific MAID crosses the "fence," advertisers can deliver personalized messaging to the mobile device in real time.

29. Geofencing also permits advertisers to gather valuable data on consumer behavior and preferences by analyzing the location-based interactions of users. In short, MAIDs can be used to match an individual’s mobile device with the locations they visited.

30. Defendant permits advertising companies to collect customer information and create unique identifiers tied to a customer’s mobile device. For example, the VZ Navigator privacy policy provides, in part, as follows:

“We disclose information to advertising companies. We may disclose, or allow certain third-party advertising companies to collect, information about your activity on our sites and in our apps. These companies may use your email address, or other *information they collect to create one or more identifiers associated with you or your device(s) both on and off our sites and in our apps.* They can use that information to help us provide more relevant Verizon advertising on our own and third-party sites and apps. *These companies may combine this information with information they collect elsewhere to determine whether you or someone with similar interests may fit into an audience that advertisers, including Verizon, are trying to reach, to serve targeted advertising to you on our sites and other sites and platforms, or to find other potential customers.* To do this, we and these companies use a variety of tracking, validation and other technologies, such as cookies, pixels, web beacons, tags, scripts, or similar technologies on our pages and the browsers you use, or we *may disclose information using application programming interfaces (APIs)* Verizon sites and services may also include social networks or other third-party plug-ins and widgets that may provide information to their associated social networks or third parties even if you do not click on or otherwise interact with the plug-ins and widgets.

31. Upon information and belief, these advertisers analyze the location data attached to a customer’s MAID to categorize the customer into audience segments based on similar interests or characteristics revealed by the customer’s use of their mobile device.

32. Upon information and belief, Defendant also disclosed CPNI to third-party advertisers using application programming interfaces (APIs).¹ For example, a mobile app might use an API to retrieve user-related data from a server or to send user interactions back to the server.

¹APIs allow different apps to share information with each other. App developers use existing APIs provided by other companies to access data or features without needing to know how the code works.

33. APIs often access location information, and this capability is commonly used in various applications and services such as:

- a. **Geolocation APIs**—these allow applications to retrieve the user’s current location based on GPS, Wi-Fi, or cellular data.
- b. **Geocoding APIs**—these allow access to location data and provide features like directions, nearby places, and can convert an address into latitude and longitude coordinates, or Place ID, or vice versa.
- c. **Social Media APIs**—these allow access to user location data to enhance posts, enable check-ins, serve advertisements, and personalize content.
- d. **Event and Activity APIs**—these provide information about local events or activities based on the user’s location.
- e. **Advertising APIs**—these allow companies to create and manage ads, generate leads, create ad groups based on keywords, and use location information to send special offers when a user is near a specific store.

34. Upon information and belief, the primary purpose of the Defendant’s use of APIs was to enable instantaneous delivery of advertisements directly to customers’ mobile devices, such as when scrolling through a webpage or using a mobile app.

35. APIs facilitate real-time bidding on ad inventory, where advertisers can instantly evaluate and bid on ad placements based on user data like ad impressions, spend, age, gender, and event or location.

36. The API collects the customer’s personal information from their mobile device and transfers it to the bidding exchange in the form of a bid request. Among other information, the bid request typically contains the customer’s MAID and precise geolocation information, if the consumer had location sharing turned on.

37. Then, in an auction that occurs without the customer’s knowledge or involvement, advertisers bid to place advertisements based on the personal information contained in the bid request. Advertisers can view and collect the customer information contained in the bid request even when they do not have a winning bid.

38. Upon information and belief, in addition to the location and other customer information Defendant disclosed through APIs, these advertisers also purchased customer information from data brokers and other companies that collect customer information from other sources. By collecting data in this manner, advertisers can use technical measures like machine learning and artificial intelligence to connect the information collected through other means with the information retrieved from the APIs, and ultimately identify individual customers.

39. Through the software preloaded onto its smartphones, tablets, smart watches, websites, and mobile apps, Defendant disclosed customer information it obtained by virtue of the carrier-customer relationship to advertising companies without obtaining prior consent.

40. Defendant's collection and use of data retrieved from mobile devices (and other sources) was unclear to its customers, who typically are unaware of the mobile advertising ecosystem. Especially considering these actions take place "in the background" beyond the perception of the average customer.

41. Once information is collected from mobile devices and/or other sources, the information can be, and in many instances is, redisclosed multiple times to other companies that the customer has never interacted with.

42. Customers have no understanding of how the information collected about them can be used to surveil their movements or that inferences about them and their behaviors can be drawn from this information. Since Defendant's customers are automatically included in this process, Plaintiff and Class Members were unable to take reasonable steps to prevent the unauthorized disclosure of their CPNI.

[B] Defendant's unauthorized disclosure of customer information for targeted advertising requires the expenditure of time and/or money to investigate and remedy the breach.

43. The invasion of Plaintiff's and Class Members' privacy as described herein constitutes an actual, particularized, redressable injury traceable to the Defendant's conduct.

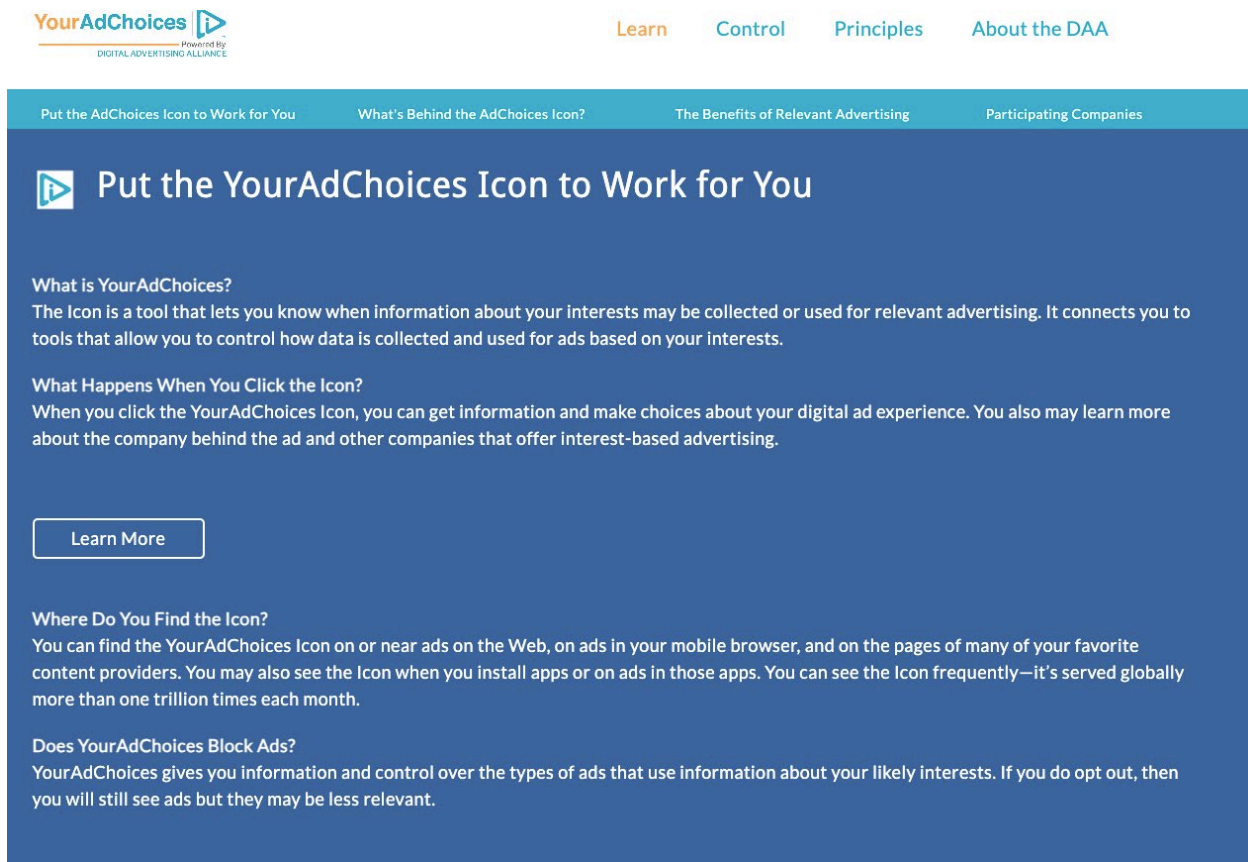
44. Defendant disclosed and/or sold information to unauthorized third parties about how its customers used their mobile devices, including, but not limited to, device location, app/feature use, IP address, device type and amount of use.

45. To prevent Defendant from collecting and using network location information, specifically, customers could only turn their devices off because the operating system on their mobile device *automatically collects location information and discloses it to various apps*.

46. However, to enable certain in-app features, mobile apps routinely request and receive permission from users to access their location information. Unfortunately, by allowing these apps to access their location information for those in-app features, the user unwittingly enabled Defendant to collect and disclose their location data to advertisers through API calls.

47. Defendant does not provide customers any specific detail about which apps receive their location data, only that the customer will need to toggle location settings to "off" within the specific apps. Alternatively, customers can toggle device location settings to "off," which could prevent some applications from functioning properly.

48. To opt-out of the sale and sharing of their MAIDs, device identifiers, and other location information for interest-based advertising, customers were required to visit the Digital Advertising Alliance (DAA) opt-out webpage to learn more (youradchoices.com/learn).



YourAdChoices Powered by
DIGITAL ADVERTISING ALLIANCE

[Learn](#) [Control](#) [Principles](#) [About the DAA](#)

[Put the AdChoices Icon to Work for You](#) [What's Behind the AdChoices Icon?](#) [The Benefits of Relevant Advertising](#) [Participating Companies](#)

Put the YourAdChoices Icon to Work for You

What is YourAdChoices?
The Icon is a tool that lets you know when information about your interests may be collected or used for relevant advertising. It connects you to tools that allow you to control how data is collected and used for ads based on your interests.

What Happens When You Click the Icon?
When you click the YourAdChoices Icon, you can get information and make choices about your digital ad experience. You also may learn more about the company behind the ad and other companies that offer interest-based advertising.

[Learn More](#)

Where Do You Find the Icon?
You can find the YourAdChoices Icon on or near ads on the Web, on ads in your mobile browser, and on the pages of many of your favorite content providers. You may also see the Icon when you install apps or on ads in those apps. You can see the Icon frequently—it's served globally more than one trillion times each month.

Does YourAdChoices Block Ads?
YourAdChoices gives you information and control over the types of ads that use information about your likely interests. If you do opt out, then you will still see ads but they may be less relevant.

49. Unfortunately, customers who visited the YourAdChoices link could not opt-out of targeted advertising. Instead, they would be routed to a “partial list” of companies (brand advertisers, agencies, publishers, ad networks, and ad tech companies) that participate in the interest-based advertising ecosystem.

50. There are over 100 companies on the “partial” list of participating companies. However, the list contains links to third-party websites that merely contain explanations regarding how a consumer could turn off certain types of targeted advertising.

51. Unfortunately, there is no way for the customer to identify to which third parties Defendant sold or disclosed their information.

[Learn](#)[Control](#)[Principles](#)[About the DAA](#)

DAA Participating Companies & Organizations

DAA participating companies are leaders in every part of the U.S. interest-based advertising ecosystem who use consumer information responsibly for marketing purposes in accordance with DAA Principles. Those participating companies include brand advertisers, agencies, publishers, ad networks, and ad tech companies. Enforcement of the DAA Principles extends beyond participating companies to cover every company using consumer data for interest-based advertising and other covered purposes under the Principles. A partial list of DAA participating companies follows:

0-9 [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

3

[33Across](#)

A

[Acxiom](#)

[adelphic](#)

[Adform](#)

[AdGear](#)

[Adobe](#)

[Adtegrity](#)

[AdTheorent](#)

[Align Technology, Inc.](#)

[Allstate](#)

[Alphonso](#)

[Amgen](#)

[Amobee](#)

[Audiencerate](#)

[Audigent](#)

B

[Bank of America](#)

[Basis Technologies](#)

[Bayer](#)

[Tremor Video](#) | [Nexxen](#)

U

[Undertone](#)

[University of Phoenix, Inc.](#)

[Unruly](#)

[UNTU, LLC](#)

V

[VDX.TV](#)

[Vericast](#)

[Verizon](#)

[Viant Inc.](#)

[ViralGains.com](#)

[Voya](#)

W

[The Weather Channel](#)

[Weather Underground](#)

[WebMD](#)

[Wells Fargo](#)

[Western Union](#)

X

[Xaxis](#)

Y

[Yahoo!](#)

[Yieldmo, Inc.](#)

Z

[Zeta Global](#)

[Ziff Davis](#)

52. Although “Verizon” is listed, clicking on the link only rerouted the customer back to the Verizon webpage. This is circular and does not resolve the issues caused by Defendant’s unauthorized conduct.

53. For mobile devices, specifically for Android devices, customers were required to opt-out using the settings on *each* smartphone, tablet, smart watch, or other wireless-enabled device for which they no longer wished to receive targeted advertisements. Going through each mobile app, on each device, to identify which apps access location data and/or which apps use location data to administer targeted advertisements would require a significant expenditure of time (and a level of technical knowledge that many users do not have).

54. Even if Plaintiff and Class Members were able to identify which advertisers received their information, reviewing each company’s respective privacy policy and following the opt-out and deletion procedures, if any, would require a significant expenditure of time.

55. Furthermore, Plaintiff and Class Members are completely unaware of the data brokers/aggregators that have purchased or accessed their CPNI as a result of this mobile advertising scheme. As mentioned previously, there are over 100 companies on the Digital Advertising Alliance’s “partial” list of participating companies. The process of removing Plaintiff and Class Members’ data can take several days or weeks and the process may need to be repeated periodically.

56. As a direct result of the unauthorized disclosure of their information, Plaintiff and Class Members are now required to spend effort and resources finding and removing their information from the internet, which involves: (a) scanning data broker websites to find records; (b) performing “opt-outs” on each data broker website; (c) confirming the data removal request by email; (d) submitting completed PDF forms; (e) receiving confirmation codes and submitting them

to the data broker websites; (f) continued scanning of the data broker websites to confirm removal of personal data; and (g) regularly monitoring all data broker websites to detect reappearing records.

57. Alternatively, Plaintiff and Class Members may automate the opt-out process. For example, the cost to automate this opt-out process can cost \$355.32 a year or \$32.90 per month.²

58. The necessary expenditure of time and/or money required to remove data from the internet is an actual, particularized, and concrete harm, traceable to the Defendant's unauthorized disclosure of customer proprietary network information.

[C] Defendant's practice of sharing de-identified/aggregated customer information, under the circumstances, is likely to mislead its customers and/or cause them harm.

59. Upon information and belief, Defendant surveilled its customers and combined "Verizon and third-party information" to create business and marketing insights.

60. Upon information and belief, "Verizon and third-party information" included information about how its customers used their mobile device (such as web browsing, device location, app/feature use, and IP address or similar information), about products and services customers used (such as device type and amount of use), points of interest, demographic information (such as gender, age range, etc.) and location information Defendant obtained from other sources.

61. The privacy policy associated with the VZ Navigator mobile app, for example, stated, "[w]e may de-identify or aggregate information so that Verizon or others may use it for business and marketing purposes. . . . [t]he information we use and the insights we develop [from

² The annual plan reflects a 10% discount. See, IDX, Individual Consumer Plans, <https://www.idx.us/privacy-identity-protection/consumer-plans>

Verizon and third-party information] do not identify you individually and may be disclosed to third parties.”³

62. Although Defendant contends the information it uses and the insights it develops do not identify customers individually, such claims are misleading.⁴

63. Generally, “every time you release any statistic calculated from a confidential data source, you reveal, or leak, a small amount of private or confidential information.”⁵ Furthermore, each value disclosed can be used to “reduce uncertainty” regarding inferences drawn about the data subjects reflected in the dataset.⁶

64. In the context of location data, “[s]ignificant research has shown that ‘anonymized’ data can often be re-identified” and that it is “possible to uniquely identify 95% of a dataset of 1.5 million individuals using four location points with timestamps.”⁷

65. Another study found that 99.98% of Americans could be correctly re-identified in any dataset using just 15 personal attributes.⁸ Using only date of birth, location (PUMA code⁹), marital status, and gender can individually identify 78.7% of a dataset of 3 million individuals.¹⁰

³ See e.g., VZ Navigator privacy policy. The policy was available in the mobile application but cannot be reproduced here since the app has been discontinued.

⁴ Data re-identification is a growing concern as machine learning models (*i.e.*, artificial intelligence) are becoming more adept at making predictions or decisions based on patterns it identifies in an anonymized dataset.

⁵ See, Keller *et al.*, Database reconstruction does compromise confidentiality. *Proc. Natl. Acad. Sci.*, 120, e2300976120 (2023).

⁶ Keller *et al.*

⁷ See, K. Cohen, Federal Trade Commission Division of Privacy & Identity Protection, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data.*, (2022). Available here: <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal>.

⁸ See, Rocher, L., Hendrickx, J.M. & de Montjoye, YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat. Commun.*, 10, 3069 (2019). Available here: <https://www.nature.com/articles/s41467-019-10933-3#citeas>.

⁹ A Public Use Microdata Area (PUMA) code is a unique identifier used by the U.S. Census Bureau to represent geographical areas that are designed for the dissemination of statistical data. PUMA codes are used in research to allow detailed analysis of specific geographical regions without compromising individual privacy.

¹⁰ See, Rocher, L., Hendrickx, J.M. & de Montjoye, YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat. Commun.*, 10, 3069 (2019).

66. For de-identified and aggregated data to truly be confidential, there must be no residual risk that the information can be used to “re-identify any individual or device that identifies or is linked or reasonably linkable to an individual.”¹¹

67. Defendant’s collection and use of data gathered from mobile devices (and other sources) is opaque to its customers, who typically do not know what data is being collected and when, who their data is being shared with, what data is being shared, or how it is being used.

68. Making matters worse, Defendant improperly requires its customers to opt-out of this practice without providing sufficient detail to exercise informed consent (or the revocation thereof).

69. Unfortunately, Defendant’s “opt-out” approach places an “unreasonable burden on consumers by forcing them to manage confusing, innumerable, and ever-changing settings . . . *opt-out schemes routinely fail to protect consumers’ privacy* because they are difficult for consumers to use and understand (if consumers are aware of their existence to begin with). *As a result, many consumers do not exercise their opt-out rights, and those that do are often forced to expend significant time and energy to protect their privacy.*”¹²

70. Therefore, Defendant’s attempt to placate its customers’ privacy concerns by asserting the personal data it shares with third-party advertisers has been de-identified—which further reduces the chance that a customer will opt-out of these data collection practices—is an

¹¹ See, Electronic Privacy Information Center (EPIC), EPIC Comments on the CFPB’s Personal Financial Data Rights Rulemaking (Jan. 25, 2023)

¹² See, EPIC Comments on the CFPB’s Personal Financial Data Rights Rulemaking (Jan. 25, 2023), citing Hana Habib, et al., *An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites*, Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS 2019) 387-406 (2019), https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-hana_habib.pdf (“This heuristic evaluation identified substantial issues that likely make exercising these privacy choices on many websites difficult and confusing for US-based consumers. Even though the majority of analyzed websites offered privacy choices, they were located inconsistently across websites. Furthermore, some privacy choices were rendered unusable by missing or unhelpful information, or by links that did not lead to the stated choice.”).

unfair or deceptive practice that is likely to cause substantial injury to its customers. Since the Defendant's use of the CPNI at issue is not essential to the provision of a telecommunications service, and is solely for the Defendant's benefit (i.e., advertising) the injury is not outweighed by the benefits to Plaintiff and Class Members.

71. The collection and use of CPNI and other personal data in this fashion constitutes an unwarranted invasion of Plaintiff's and Class Members' privacy.

[D] Since customers were *automatically* included in the Defendant's mobile advertising practices, Defendant could not obtain valid consent for the disclosure.

72. Because Defendant did not obtain prior affirmative consent for the secondary usage of the CPNI at issue, Plaintiff and Class Members were wholly unaware that Defendant was collecting this data from their mobile devices.

73. Plaintiff and Class Members were likewise wholly unaware that Defendant would use this data to create detailed customer profiles based on interests or characteristics revealed by the location of their mobile device.

74. Valid legal consent requires the data subject to voluntarily agree to have their data processed, *after* being fully informed about how it will be used and how they can withdraw their consent.

75. Although Defendant's privacy policies disclosed the general nature of its advertising practices, such information was provided after the data collection had occurred. Furthermore, the privacy policies at issue could not "fully inform" a Class Member who attempted to opt-out of the Defendant's practices because the policies do not provide any details about what Defendant did with their data and/or permitted third parties to do with their data.

76. Likewise, Defendant did not provide clear instructions on how to request Defendant stop sharing location and other data with the advertising companies Defendant allowed to access

their mobile devices. Defendant only provided generic explanations regarding how a customer could turn off location sharing in certain mobile apps. However, there were no instructions on which mobile apps customers should submit a request to specifically.

[E] Defendant’s practices pose an unwarranted intrusion into Plaintiff’s and Class Members’ lives and has caused, or is likely to cause, substantial injury to its customers.

77. Upon information and belief, the location data and other “Verizon and third-party information” shared or sold by Defendant can be used to identify individual customers and their visits to sensitive locations, such as visits to houses of worship, political protests, abortion clinics, and doctors’ offices.

78. Using the personal information that Defendant collects, Defendant categorizes its customers into custom audience segments to allow its business and marketing clients to target groups of customers for advertising.

79. Upon information and belief, Defendant develops standard audience segments that it sells to its clients and creates custom audiences based on specific information that its clients request.

80. Upon information and belief, it is possible to identify sensitive characteristics (or to infer sensitive information from) location data associated with a customer’s MAID. Therefore, Defendant sells or produces data products that its clients can use to associate individual customers with health conditions, gender identity and sexual orientation, political activity, and religious practices, which puts Class Members at significant risk of stigma, discrimination, and other harms.¹³

¹³ See, Electronic Frontier Foundation (EFF), *Top Apps Invade User Privacy By Collecting and Sharing Personal Data, New Report Finds*, (Jan. 14, 2020) (discussing a report published by the Norwegian Consumer Council (NCC) called “Out of Control: How Consumers Are Exploited by the Online Advertising Industry”) The article and report can be access here: <https://www.eff.org/deeplinks/2020/01/new-report-exposes-adtech-invading-our-privacy>. See

81. The identification of sensitive and private characteristics of individual customers from the location data sold or disclosed by Defendant constitutes an unwarranted invasion of Plaintiff's and Class Members' privacy.

82. The imminent risk of future harm resulting from the unauthorized disclosure of CPNI is traceable to the Defendant's failure to maintain the confidentiality of the data in its custody, and has created a separate, particularized, and concrete harm to the Plaintiff and Class Members.

83. As a result of the unauthorized disclosure of their CPNI, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) lost time and opportunity costs associated with investigating and attempting to mitigate the consequences of the data breach; (iii) statutory damages; (iv) nominal damages; (v) actual damages; (vi) significant risk of stigma, discrimination, and future data breaches; and (vii) the continued and increased risk their CPNI will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

84. Plaintiff brings this class action lawsuit individually, and on behalf of all those similarly situated, to address Defendant's inadequate data protection practices.

also, report on the numerous ways U.S. and other companies profit from third-party tracking, which is available at: <https://www.eff.org/wp/behind-the-one-way-mirror>.

CLASS ACTION ALLEGATIONS

85. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), 23(c)(4), and 23(c)(5), of the Federal Rules of Civil Procedure.

86. The Class that Plaintiff seeks to represent is defined as follows:

Nationwide Class: All individuals residing in the United States and its territories whose CPNI and other personally identifiable information was collected, disclosed, and/or sold by Defendant without their knowledge or consent (the “Class”).

87. Plaintiff reserves the right to amend the definition of the Class or add a Class or Subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

88. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

89. **Numerosity:** The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. While the exact number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant, upon information and belief, more than 140 million individual wireless subscribers were impacted by Defendant’s business practices.

90. **Commonality:** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class that predominate over questions which may affect individual Class Members, includes the following:

- a. Whether and to what extent Defendant had a duty to maintain the confidentiality of Plaintiff's and Class Members' CPNI;
- b. Whether Plaintiff and Class Members consented to the disclosure of their CPNI for secondary use;
- c. Whether Defendant was unjustly enriched;
- d. Whether Defendant's conduct constitutes an invasion of privacy;
- e. Whether Defendant's conduct was negligent, willful or wanton;
- f. Whether Defendant adequately and accurately informed Plaintiff and Class Members of how their CPNI would be used before granting third parties access to said data;
- g. Whether Defendant violated the law by failing to obtain affirmative consent before disclosing location data to third party advertisers;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct, and the amount of said damages; and,
- j. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced as a result of the Data Breach.

91. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

92. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

93. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic

to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data privacy litigation, and Plaintiff intends to prosecute this action vigorously.

94. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit many Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

95. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action

alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

96. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

97. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

98. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the CPNI of the Class, and Defendant may continue to act unlawfully as set forth in this Complaint.

99. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

100. To the extent not all issues or claims, including the amount of damages, can be resolved on a class-wide basis, Plaintiff reserves the right to seek certification of a class action with respect to particular issues.

COUNT ONE: NEGLIGENT/WANTON DISCLOSURE OF CONFIDENTIAL DATA
(On Behalf of Plaintiff and the Class)

101. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

102. Defendant is a telecommunications carrier within the contemplation of the Telecommunications Act of 1996, 47 U.S.C. §222(a) and, as such, has a duty to protect the confidentiality of proprietary information of, and relating to, its customers.

103. Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of: (a) the telecommunications service from which such information is derived; or (b) services necessary to, or used in, the provision of such telecommunications service.

104. The term “telecommunications service” means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.

105. The term “customer proprietary network information” means information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.

106. The data at issue in this Complaint relates to the both the technical configuration and location of a telecommunications service.

107. Technical configuration refers to adjusting the settings of a computer, mobile device, or application by either the user or the programmer to achieve a desired function. The data at issue here relates to the specific settings and parameters that define how a wireless enabled mobile device functions, including aspects like network connectivity and installed applications. In other words, that data at issue here, relates to how the mobile device operates and interacts with Defendant’s wireless network.

108. Once a wireless enabled mobile device is attached to Defendant's wireless network, Defendant uses the device's location to enable the customer to send and receive data or calls. Therefore, when Defendant's customers access the commercial mobile service to which they subscribe, Defendant can use its network to determine the device's location.

109. Plaintiff and Class Members are customers of Defendant's telecommunications products and services. By purchasing telecommunications service from Defendant, Plaintiff and Class Members were obligated to make their device location available to Defendant.

110. To prevent Defendant from collecting and using network location information, customers could only turn their devices off because the operating system on their mobile device *automatically collects location information* and discloses it to various apps.

111. Furthermore, by nature of the customer-carrier relationship, Plaintiff and Class Members were obligated to make the "identifiers associated with [them and their] devices" available to advertising companies.

112. Defendant disclosed and/or sold information to advertising companies and/or other third parties about how customers used their mobile devices, including, but not limited to, device location, app/feature use, IP address, device type and amount of use. The disclosure of the CPNI at issue here was done without the Plaintiff and Class Members' affirmative consent.

113. By permitting the unauthorized disclosure, Defendant acted negligently and/or with a reckless disregard for the Plaintiff's and Class Members' privacy. Defendant knew, or should have known, that its failure to take reasonable precautions to protect customer information from unauthorized disclosure might result in injury to Plaintiff and Class Members.

114. Plaintiff and Class Members are within the class of persons the Telecommunications Act of 1996, 47 U.S.C. §222, was intended to protect and the type of disclosures described herein were the type of harm the statute was intended to guard against.

115. Plaintiff and the Class had no ability to protect their CPNI from disclosure. Defendant was in the best position to protect against the harms suffered by Plaintiff and the Class as a result of the unauthorized disclosure.

116. But for Defendant's breach of duties owed to Plaintiff and the Class, their CPNI would not have been compromised. As a direct and proximate result of Defendant's unlawful disclosure, Plaintiff and Class Members were harmed and caused to lose the confidentiality of their sensitive data, which has caused Plaintiff and Class Members to suffer mental anguish, actual damages, loss of expenses and time spent erasing their data from the internet, and an invasion of their privacy in an amount to be determined at trial.

117. Unless enjoined and restrained by order of this Court, Defendant's wrongful conduct will cause irreparable injury to the Class as their CPNI, and any inference drawn therefrom, may be distributed and used by countless unknown third parties in the future.

118. Plaintiff and Class Members seek nominal, compensatory, and punitive damages as a result of Defendant's actions. Plaintiff and Class Members also seek actual damages, plus any profits attributable to Defendant's use of their data for advertising, marketing, business insights, or any other unauthorized use.

119. Punitive damages are appropriate because Defendant's actions were done in conscious disregard for Plaintiff's and Class Members' privacy rights and to deter future misconduct.

COUNT TWO: UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

120. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

121. By unknowingly providing their CPNI to Defendant for advertising purposes, Plaintiff and Class Members conferred a monetary benefit on Defendant. Defendant knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit.

122. Before using the CPNI as described herein, Defendant was obligated to keep such information confidential, to adequately notify Plaintiff and Class Members of the proposed uses of their CPNI and obtain affirmative consent for such uses.

123. Defendant failed to secure Plaintiff's and Class Members prior consent; therefore, it would be unjust for Defendant to retain any of the benefits that Plaintiff and Class Members conferred upon Defendant without paying value in return.

124. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) lost time and opportunity costs associated with investigating and attempting to mitigate the consequences of the data breach; (iii) statutory damages; (iv) nominal damages; (v) actual damages; and (vi) the continued and increased risk their CPNI will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

125. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

COUNT THREE: INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

126. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

127. Plaintiff and Class Members had a legitimate expectation of privacy in their CPNI and other personally identifying information. Plaintiff and Class Members were entitled to the protection of this information from disclosure to unauthorized third parties.

128. Defendant owed a duty to Plaintiff and Class Members to keep their CPNI confidential. However, Defendant permitted the public disclosure of Plaintiff's and Class Members' CPNI to unauthorized third parties through the use of cookies, pixels, web beacons, tags, scripts, MAIDs, APIs, or similar technologies.

129. As Plaintiff and Class Members used their mobile devices, Defendant permitted the surreptitious collection of highly sensitive data mapping their personal lives, which is then analyzed and sold without their knowledge or informed consent.

130. The CPNI that was disclosed without the Plaintiff's and Class Members' authorization was highly sensitive, private, and confidential. The public disclosure of the type of data at issue here would be highly offensive to a reasonable person of ordinary sensibilities.

131. Despite knowledge of the substantial risk of harm created by collecting sensitive data, Defendant intentionally disregarded the risk, thus permitting the invasion of Plaintiff's and Class Members' privacy for profit.

132. Defendant's conduct was highly offensive to a reasonable person considering the scientific literature, articles, enforcement actions, and advocacy groups' attention and effort to protect consumers from this manner of surveillance.

133. By facilitating these unauthorized disclosures, Defendant acted with reckless disregard for the Plaintiff's and Class Members' privacy, and with knowledge that such disclosure would be highly offensive to a reasonable person. Furthermore, the disclosure of the data at issue was not newsworthy or of any service to the public interest.

134. Defendant was aware of its duty to detect and to prevent the unauthorized disclosure of Plaintiff's and Class Members' data.

135. Defendant acted with such reckless disregard as to the safety of Plaintiff's and Class Members' CPNI to rise to the level of intentionally allowing the intrusion upon the seclusion, private affairs, or concerns of Plaintiff and Class Members.

136. As a direct and proximate result of Defendant's unlawful disclosure, Plaintiff and Class Members were harmed and caused to lose the confidentiality of their sensitive data, which has caused Plaintiff and Class Members to suffer mental anguish, actual damages, loss of expenses and time spent erasing their data from the internet, and an invasion of their privacy in an amount to be determined at trial.

137. Unless enjoined and restrained by order of this Court, Defendant's wrongful conduct will cause irreparable injury to the Class as their CPNI, and any inference drawn therefrom, may be distributed and used by countless unknown third parties in the future.

138. Plaintiff and Class Members seek nominal, compensatory, and punitive damages as a result of Defendant's actions. Plaintiff and Class Members also seek actual damages, plus any

profits attributable to Defendant's use of their data for advertising, marketing, business insights, or any other unauthorized use.

139. Punitive damages are appropriate because Defendant's actions were done in conscious disregard for Plaintiff's and Class Members' privacy rights and to deter future misconduct.

COUNT FOUR: VIOLATION OF THE FEDERAL WIRETAP ACT

(On Behalf of Plaintiff and the Class)

140. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

141. Under 18 U.S.C. §2511(1)(a), Defendant is prohibited from intentionally intercepting, or procuring any other person to intercept, any wire, oral, or electronic communication.

142. Furthermore, Defendant is prohibited from intentionally disclosing to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication. 18 U.S.C. §2511(1)(c).

143. Also prohibited is the intentional use of the contents of any wire, oral, or electronic communication, while knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication. 18 U.S.C. §2511(1)(d).

144. The term "intercept" means the acquisition of the contents of any wire, electronic, or oral communication using any electronic, mechanical, or other device. 18 U.S.C. §2510(4).

145. The term "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,

electromagnetic, photoelectronic or photo-optical system that affects interstate or foreign commerce. 18 U.S.C. §2510(12).

146. Plaintiff and Class Members bring this count against Defendant because their wire, oral, or electronic communications have been intercepted, disclosed, or intentionally used in violation of the Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986 by Defendant, or unknown third parties acting on Defendant's behalf. 18 U.S.C. §2520(a).

147. Defendant, or third-party companies acting on Defendant's behalf, intentionally intercepted electronic communications regarding its customers mobile devices using cookies, pixels, web beacons, tags, scripts, APIs, or similar technologies.

148. Defendant intentionally disclosed the contents of the electronic communications it intercepted from Plaintiff's and Class Member's mobile devices to business partners, marketing clients, and advertisers, while knowing such information was obtained through the interception of a wire, oral, or electronic communication.

149. Defendant intercepted, in real time, the contents of electronic communications transmitted to, within, and from Plaintiff's and Class Members' mobile devices and apps, and then diverted those communications to themselves and other third-parties without consent.

150. More specifically, Defendant intentionally used, disclosed, permitted access to, and/or sold the contents of electronic communications it intercepted about its customers use of their mobile device (such as web browsing, device location, app/feature use, and IP address, device type, MAID, points of interest, and demographics) to develop targeted advertisements, and business and marketing insights.

151. As stated earlier herein, Defendant disclosed or permitted third-party advertising companies to collect one or more identifiers associated with and connected to individual customers

and their mobile devices. Plaintiff and Class Members have a reasonable expectation of privacy in their CPNI as such data is required to be kept confidential. More specifically, Plaintiff and Class Members have a reasonable expectation of privacy with respect to the sensitive data that can be collected (or the inferences drawn therefrom) using geolocation data.

152. Plaintiff and Class Members have suffered harm and injury due to the intentional interception, disclosure, and/or use of electronic communications containing their sensitive personal information.

153. As a direct and proximate result of Defendant's unlawful interception, disclosure, and/or use of their protected communications, Plaintiff and Class Members were harmed and are entitled to appropriate relief such as: (a) equitable or declaratory relief as may be appropriate; (b) reasonable attorney's fee and other litigation costs reasonably incurred; (c) monetary damages, in an amount to be determined at trial, assessed as the greater of (i) the sum of the actual damages suffered by the Plaintiff and Class, plus any profits made by Defendant as a result of its violation; or (ii) statutory damages to each Class Member, of whichever is the greater of \$100.00 a day for each day of violation or \$10,000.00.

COUNT FIVE: VIOLATION OF THE COMPUTER FRAUD & ABUSE ACT

18 U.S.C. §§1030, *et seq.*

(On Behalf of Plaintiff and Class Members)

154. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

155. The Computer Fraud & Abuse Act prohibits Defendant from knowingly accessing a computer without authorization, or exceeding authorized access, and obtaining, by means of such access, information from any protected computer.

156. The term “protected computer” means a computer which is used in or affecting interstate commerce or communication. 18 U.S.C. §1030(e)(2). The term “computer” means an electronic or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any communications facility directly related to or operating in conjunction with such device. 18 U.S.C. §1030(e)(1).

157. Plaintiff’s and Class Members’ mobile devices (e.g., smartphones, tablets, smart watches) are computers within the meaning of the statute.¹⁴ As “mobile” devices they are also purchased in and/or used for interstate commerce or communication within the meaning of the statute.

158. Defendant intentionally accessed Plaintiff’s and Class Members’ protected mobile devices to obtain, by virtue of such access, information pertaining to their use of said devices, such as web browsing history, device location, app/feature use, and IP address. Defendant either did so without consent, or Defendant’s conduct exceeded authorized access by obtaining information from the mobile device that Defendant was not expected or entitled to obtain.

159. Through Defendant’s use of cookies, pixels, web beacons, tags, scripts, APIs, or similar technologies embedded in its network, websites and mobile apps, Defendant intentionally accessed the Plaintiff’s and Class Members’ mobile devices without authorization or in a manner that exceeded the Plaintiff’s and Class Members’ authorization and obtained information therefrom in violation of the statute.

¹⁴ See, National Institute of Standards and Technology (NIST), defining a mobile device as a “portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations.

160. Plaintiff and Class Members have suffered loss due to Defendant's unauthorized access to the communications containing their confidential and sensitive information and Defendant's sale or disclosure of such information to third parties for targeted advertising.

161. The Defendant was required by law to obtain prior affirmative consent to disclose the data at issue herein, and by using the data for its own purposes unrelated to the provision of a telecommunications service, it either exceeded authorization or never obtained authorization for such use. Through the fraudulent concealment of its business practices, Defendant obtained valuable data from protected computers.

162. Upon information and belief, the value of the information obtained and/or the loss to Plaintiff and the Class, during any 1-year period, exceeded \$5,000.00 in the aggregate.

163. As a direct and proximate result of Defendant's unlawful conduct, Plaintiff and Class Members are entitled to appropriate relief such as: (a) equitable or declaratory relief as may be appropriate; (b) reasonable attorney's fee and other litigation costs reasonably incurred; (c) statutory relief, and (d) monetary damages, in an amount to be determined at trial.

**COUNT SIX: VIOLATION OF GEORGIA'S UNIFORM DECEPTIVE TRADE
PRACTICES ACT {OCGA § 10-1-370 et seq.,}
(On Behalf of Plaintiff)**

164. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

165. Plaintiff is a customer of Defendant and has purchased Defendant's products and services. Defendant requires its customers, including Plaintiff, to submit CPNI in the ordinary course of providing telecommunications services.

166. Defendant surreptitiously collected and shared, or permitted the surreptitious collection of, the Plaintiff's CPNI as part of its advertising, business, and marketing insights

programs. Defendant represented that the information it used and the insights it developed did not individually identify a wireless customer. More specifically, Defendant contends that it “may de-identify or aggregate information so that Verizon or others may use it for business and marketing purposes.”

167. Section 5 of the Federal Trade Commission Act, 15 U.S.C. §45 prohibits unfair or deceptive trade practices that affect commerce. Deceptive practices, as interpreted by the FTC, include making false claims regarding the de-identification of data. Such behavior also constitutes a false, misleading, or deceptive act under Georgia’s Uniform Deceptive Trade Practices Act OCGA § 10-1-370 *et seq.*

168. Upon information and belief, Defendant violated the statute by making false claims about data anonymization, misusing the CPNI it collected, and failing to maintain the confidentiality of Plaintiff’s information.

169. As a result of the Defendant’s false, misleading, or deceptive acts, Plaintiff suffered injuries including, but not limited to: (i) invasion of privacy; (ii) lost time and opportunity costs associated with investigating and attempting to mitigate the consequences of the data breach; (iii) statutory damages; (iv) nominal damages; (v) actual damages; and (vi) the continued and increased risk their CPNI will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant’s possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

170. Plaintiff is entitled to appropriate relief such as: (a) equitable or declaratory relief; (b) reasonable attorney’s fee and other litigation costs reasonably incurred; and (c) monetary damages, in an amount to be determined at trial.

COUNT SEVEN: DECLARATORY RELIEF

(On Behalf of Plaintiff and the Class)

171. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

172. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

173. An actual controversy has arisen in the wake of Defendant's unauthorized disclosure of CPNI for purposes of advertising and regarding Defendant's present and prospective duties to reasonably safeguard its customers' data obtained from their mobile devices.

174. Plaintiff alleges that Defendant's opt-out scheme for mobile advertising routinely fails to protect its customer's privacy because it is difficult for customers to use and understand. As such, many customers remain unaware of their rights, do not exercise their opt-out rights, and those that do, are forced to expend significant time and effort to protect their privacy.

175. As a result, Plaintiff and the Class will continue to suffer injury as a result of the misuse of their CPNI and remain at imminent risk that further compromises of their CPNI will occur in the future.

176. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendant continues to owe a legal duty to discover and protect against unauthorized disclosures of CPNI, especially as it relates to the mobile advertising ecosystem.
- b. Defendant continues to breach this legal duty by employing the opt-out scheme.

- c. That secondary uses of CPNI, other than those reasonably necessary to provide a requested product or service, are prohibited without obtaining the prior consent of the customer.
- d. Prohibiting the use of CPNI that has been nominally de-identified from being used or disclosed to third parties for secondary uses, such as marketing and advertising.
- e. Requiring the disclosure of essential information to customers about what third parties are permitted access to their CPNI and the purpose of the disclosure, prior to the data being used for marketing and advertising.

177. The Court also should issue corresponding prospective injunctive relief requiring that Defendant employs adequate data protection practices consistent with law and industry standards such as providing tangible privacy rights for customers, including the right to know, the right to data portability, and the right to delete data previously collected.

178. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another unauthorized disclosure. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

179. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Among other things, the unauthorized disclosure of sensitive data, will likely subject Plaintiff to fraud, discrimination, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data protection measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

180. The issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by encouraging Defendant to take necessary action to prevent further unauthorized collections and disclosures, thus

eliminating the additional injuries that would result to Plaintiff and the millions of individuals whose CPNI would be at risk of future unauthorized disclosures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class alleged herein, respectfully requests that the Court enter judgment as follows:

- A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff(s) as the representatives for the Class and counsel for Plaintiff(s) as Class Counsel;
- B. For an order declaring the Defendant's conduct violates the statutes and causes of action referenced herein;
- C. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- D. For actual, compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;
- E. For prejudgment interest on all amounts awarded;
- F. For an order of restitution and all other forms of equitable monetary relief requiring the disgorgement of the revenues wrongfully retained as a result of the Defendant's conduct;
- G. For injunctive relief as pleaded or as the Court may deem proper; and
- H. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and
- I. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated: February 6, 2025

Respectfully submitted,

SULTZER & LIPARI, PLLC

/s/ Philip J. Furia

By: _____

Philip J. Furia, Esq.
Jason P. Sultzer, Esq.
85 Civic Center Plaza, Suite 200
Poughkeepsie, NY 12601
Tel: (845) 483-7100
furiap@thesultzerlawgroup.com
sultzerj@thesultzerlawgroup.com

-AND-

Paul J. Doolittle, Esq.*
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
cmad@poulinwilley.com

Attorneys for Plaintiff

**Pro Hac Vice forthcoming*